



Daily Cyber Headlines

Daily Cyber Headlines

☐ TLP:WHITE

Alert ID : 80261a52

Oct 01, 2026, 04:16 AM



Today's Headlines:

Leading Story

- Cisco Warns of New SD-WAN Zero-Day Exploited in Attacks

Data Breaches & Data Leaks

- Arrowhead Regional Medical Center Data Breach

Cyber Crimes & Incidents

- Russia's Star Blizzard Targets 100+ Organizations with Fake Event Invites to Deliver Backdoor
- Cyber Risks of Democratic People's Republic of Korea IT Workers to New Zealand Organizations

Vulnerabilities & Exploits

- WatchGuard Patches Critical Fireware OS Code Injection Vulnerability
- TeamViewer Urges Users to Patch Critical Flaws

Trends & Reports

- Vulnerability Discovery and Exploitation Trends in the AI Era

Privacy, Legal & Regulatory

- Nothing To Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
 - APAC – October 02, 2026, 01:00-02:00 PM AEST
 - Americas – October 27, 2026, 12:00 PM - 1:00 PM ET
 - European – October 28, 2026, 03:00-04:00 PM CET

Additional Information

Leading Story

Cisco Warns of New SD-WAN Zero-Day Exploited in Attacks

Summary

- A zero-day in Cisco Catalyst SD-WAN Manager is being actively exploited to bypass API authentication and obtain administrator privileges. The flaw affects vulnerable deployments regardless of configuration, with security updates available and no complete workaround.

Analysis & Action

CVE-2026-76504, rated CVSS 9.8, is a critical authentication bypass vulnerability affecting Cisco Catalyst SD-WAN Manager, formerly known as SD-WAN vManage. The vulnerability affects deployments regardless of system configuration and allows an unauthenticated remote attacker to access the management API with administrator privileges. Active exploitation was identified in September 2026. For more information, Health-ISAC [published](#) an advisory for this.

The flaw stems from improper handling of URI encoding in HTTP requests, allowing crafted requests to bypass authentication rules that protect a specific API endpoint. Observed exploitation uses encoded characters such as %6a in requests associated with `j_security_check`. Organizations can review `serviceproxy-access.log` and `vmanage-server.log` for suspicious requests originating from unknown or unauthorized IP addresses. Details regarding the responsible threat actors and the scope of exploitation have not been disclosed.

Health-ISAC advises its members to identify affected Cisco Catalyst SD-WAN Manager deployments and upgrade immediately to an appropriate fixed release, as no workaround fully addresses the vulnerability. Organizations should restrict management

access from the internet, preserve relevant logs and forensic data before remediation, review published indicators for evidence of exploitation, and investigate potentially compromised appliances before returning them to normal operation.

Data Breaches & Data Leaks

Arrowhead Regional Medical Center Data Breach

Summary

- Arrowhead Regional Medical Center notified patients of a third-party data security incident involving its outside law firm, Buchalter, LLP, in which the unauthorized acquisition of data may have exposed personal information of certain ARMC patients.

Analysis & Action

Buchalter, LLP, an outside law firm providing legal services to Arrowhead Regional Medical Center (ARMC), discovered on August 28, 2026, that a limited amount of its data had been acquired without authorization. An investigation on September 4 determined that the affected dataset contained information belonging to certain ARMC patients, prompting coordination between Buchalter and ARMC to identify affected individuals and issue notifications.

The potentially affected information includes patient names combined with additional personal data elements that vary by individual. A complete universal list of exposed data categories has not been publicly disclosed. Buchalter described the incident as isolated and reported no evidence that the unauthorized actor accessed or affected its broader network or systems. There is also currently no evidence that affected patient information has been viewed by another party or misused.

Health-ISAC advises its members to assess third-party legal, professional services, and other vendors that receive or maintain patient information, and to ensure that appropriate security and data-handling requirements are established. Organizations should minimize the sensitive information shared with external providers, maintain visibility into third-party data access, establish coordinated breach-notification procedures, and regularly review vendors' security controls and incident-response capabilities.

Cyber Crimes & Incidents

Russia's Star Blizzard Targets 100+ Organizations with Fake Event Invites to Deliver Backdoor

Summary

- Star Blizzard has expanded phishing operations targeting more than 100 organizations, using fake event invitations and a new RedFlick delivery technique to deploy the CosmicPulse backdoor against organizations primarily in the United States and the United Kingdom.

Analysis & Action

Russian state threat actor Star Blizzard has expanded from highly targeted spear-phishing to larger campaigns involving tens to hundreds of emails. Since January 2026, at least 13 large-scale campaigns have targeted Ukrainian individuals and institutions, NGOs, think tanks, governments, financial institutions, and organizations supporting Ukraine, affecting more than 100 organizations primarily in the United States and the United Kingdom.

The campaigns commonly begin with legitimate-looking event invitations and continue only after recipients respond, at which point targets may receive password-protected RAR or ZIP archives containing malicious files. The RedFlick infection chain uses LNK files disguised as PDFs and MSI installers to establish scheduled tasks, communicate with command-and-control infrastructure, and ultimately deploy the Python-based CosmicPulse backdoor. The technique reduces the infection process to a single user interaction compared with previously observed ClickFix-based delivery methods.

Health-ISAC advises its members to strengthen defenses against conversation-based phishing by validating unexpected event invitations and follow-up attachments through trusted communication channels. Organizations should monitor for suspicious LNK, MSI, PowerShell, SSH, and WebDAV activity, hunt for RedFlick-related scheduled tasks and published indicators, restrict unnecessary outbound connections, and use phishing-resistant authentication to reduce the risk of credential and session theft.

Cyber Risks of Democratic People's Republic of Korea IT Workers to New Zealand Organizations

Summary

- DPRK IT workers are using false identities, fabricated employment histories, AI-assisted interviews, VPNs, and remote-access tools to obtain legitimate

employment, creating risks of unauthorized access, intellectual property theft, data extortion, sanctions exposure, and insider compromise.

Analysis & Action

DPRK IT workers have sought and secured employment with organizations in New Zealand and overseas, often targeting remote software development and IT roles. The advisory states that these workers form part of a state-sponsored strategy intended to generate revenue and gather intelligence, while some may seek access to proprietary information or steal organizational data for ransom.

Common techniques include stolen or purchased identities, fabricated CVs and references, deepfake or AI-assisted interview responses, VPNs and remote desktop software to conceal geographic location, and coordination through platforms such as GitHub, Telegram, LinkedIn, and Upwork. Warning indicators include inconsistent identity information, refusal to appear on camera, unusual working hours, hardware delivery addresses that differ from identity documents, logins from multiple countries, and requests for cryptocurrency or third-party payments.

Health-ISAC advises its members to strengthen identity verification and background checks for remote employees and contractors, independently validate employment, education, location, and payment information, and require the use of managed corporate devices before granting system access. Organizations should enforce least-privilege permissions, monitor VPN and remote desktop activity for geographic anomalies, review existing remote workers for multiple indicators of identity manipulation, and investigate suspicious account, payment, or access behavior.

Vulnerabilities & Exploits

WatchGuard Patches Critical Firewall OS Code Injection Vulnerability

Summary

- WatchGuard patched 15 Firewall OS vulnerabilities, including the critical CVE-2026-86131, which could allow a malicious remote VPN server to execute root-level commands on connected Firebox appliances. No exploitation has been observed in the wild.

Analysis & Action

CVE-2026-86131, rated CVSS 9.2, is a critical code injection vulnerability affecting how Firewall OS handles Branch Office VPN (BOVPN) over TLS client configurations.

Successful exploitation requires an attacker to control the remote VPN server and could allow arbitrary commands to execute with root privileges on a Firebox appliance, establishing the connection. For more information, Health-ISAC [published](#) an advisory for this.

The latest security updates address 14 additional Fireware OS vulnerabilities, including 13 high-severity flaws that could lead to remote code execution, authorization bypass, denial-of-service, unauthorized SSLVPN access, and arbitrary local file reads. Several can be exploited remotely without authentication. WatchGuard stated that it is not aware of any of the newly disclosed vulnerabilities being exploited in the wild.

Health-ISAC advises its members to identify WatchGuard Firebox appliances running affected Fireware OS versions and prioritize upgrades to 2026.3.2, 2026.2.3, 12.12.3, or 12.5.21 as applicable. Organizations should review VPN and management configurations, restrict administrative interfaces to trusted networks, monitor appliances for anomalous activity, and ensure perimeter security devices remain within supported patching lifecycles.

TeamViewer Urges Users to Patch Critical Flaws

Summary

- TeamViewer patched five high-severity vulnerabilities affecting its remote access software across Windows, Linux, and macOS. The flaws could enable remote code execution, unauthorized remote actions, arbitrary file writes, or privilege escalation on vulnerable systems.

Analysis & Action

TeamViewer disclosed five vulnerabilities affecting its Full Client, Host, and related services, with severity ratings reaching CVSS 8.8. The most critical of the five vulnerabilities, tracked as CVE-2026-92370, is an improper access control vulnerability that could allow a remote attacker to bypass user-configured permission restrictions during session establishment and perform unauthorized actions, potentially resulting in remote code execution. For more information, Health-ISAC [published](#) an advisory for this.

The remaining vulnerabilities include CVE-2026-19743, a path traversal flaw that enables arbitrary file writes with elevated privileges; CVE-2026-92368, a heap-based buffer overflow involving malicious TeamViewer session recording files; CVE-2026-92369, a Windows installer race condition that enables SYSTEM-level privilege escalation; and CVE-2026-92371, a Linux path validation issue that can enable

privileged file operations. TeamViewer reported no known public disclosure or active exploitation of the vulnerabilities at the time of publication.

Health-ISAC advises its members to identify TeamViewer Full Client and Host installations and update affected systems to version 15.82 or the latest supported maintenance or legacy release. Organizations should prioritize systems used for unattended or privileged remote access, restrict TeamViewer access to authorized personnel, review remote session activity for anomalies, and ensure remote administration software is included in endpoint inventory and vulnerability management processes.

Trends & Reports

Vulnerability Discovery and Exploitation Trends in the AI Era

Summary

- AI is reshaping vulnerability discovery and exploitation, with disclosures doubling during 2026 and AI-assisted research identifying proportionally more impactful flaws. Meanwhile, threat actors are increasingly weaponizing high-risk vulnerabilities following public disclosure.

Analysis & Action

Vulnerability disclosures increased from 5,045 in January 2026 to 10,740 in August, while observed exploitation rose from an average of 10.5 vulnerabilities per month in 2025 to 18 per month in 2026. Despite this growth, only 0.23% of disclosed vulnerabilities were observed being actively exploited, reinforcing the importance of prioritizing vulnerabilities based on real-world threat intelligence rather than disclosure volume alone.

AI-assisted vulnerability research is also producing potentially higher-impact findings. Half of the vulnerabilities identified as AI-discovered resulted in remote code execution, compared with 26% across the broader vulnerability ecosystem. At the same time, rapid weaponization of known vulnerabilities is emerging as a significant concern, while the AI operational stack itself is expanding the attack surface, with more than 1,500 AI-related vulnerabilities identified during the first eight months of 2026.

Health-ISAC advises its members to prioritize vulnerability remediation based on active exploitation, asset exposure, business criticality, and threat intelligence, rather than relying solely on vulnerability counts or severity scores. Organizations should closely

monitor internet-facing and edge infrastructure, accelerate remediation of high-risk n-day vulnerabilities, secure AI orchestration and agent frameworks, sandbox autonomous AI workloads, and incorporate AI-assisted security testing into secure development processes with appropriate human validation.

Privacy, Legal & Regulatory

Nothing to report.

Health-ISAC Cyber Threat Level

On August 20, 2026, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and decided to raise it to **Yellow (Elevated)**. The Threat Level of **Yellow (Elevated)** is due to threats from:

Critical Infrastructure Threats, ShinyHunters Activity, Ransomware Trends, AiTM Payroll Phishing, and DPRK IT Worker Fraud.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

**You must have Cyware Access to reach the Threat Advisory System document.
Contact membership@h-isac.org for access to Cyware.**

Report Source(s)

Health-ISAC

Reference

[classactionu](#)
[cyware](#)
[bleepingcomputer](#)
[securityweek](#)
[cyware](#)
[google](#)
[thehackernews](#)
[ncsc](#)
[bleepingcomputer](#)
[cyware](#)

Tags

CVE-2026-92371, CVE-2026-92370, CVE-2026-92369, CVE-2026-92368, CVE-2026-19743, CVE-2026-86131, CVE-2026-76504, WatchGuard Fireware OS, WatchGuard, DPRK IT Workers, Artificial Intelligence (AI), Star Blizzard, TeamViewer, Cisco

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Content Powered by BLACKWIRE Labs:

**Access the Health-ISAC Threat Intelligence Portal:**

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments:

Please email us at toc@h-isac.org